UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/037,560	01/04/2002	Eyal Dotan	8221-84872	7101

23493 7590 03/30/2007

SUGHRUE MION, PLLC
401 Castro Street, Ste 220
Mountain View, CA 94041-2007

EXAMINER	
HOFFMAN, BRANDON S	
ART UNIT	PAPER NUMBER
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/30/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 10/037,560	**Applicant(s)** DOTAN, EYAL	
	Examiner Brandon S. Hoffman	**Art Unit** 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 January 2007*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,8-16,19,21,23,24 and 26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8-16,19,21,23,24 and 26* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-6, 8-16, 19, 21, 23, 24, and 26 are pending in this action.

2. Applicant's arguments, filed January 18, 2007, have been fully considered but they are not persuasive.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this rejection can be found in a prior Office action.

Claim Rejections - 35 USC § 103

4. Claims 1-6, 8-16, 19, 21, 23, 24, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Keronen (U.S. Patent No. 6,871,277) in view of Edwards et al. (U.S. Patent No. 6,549,521).

Regarding claim 1, Keronen teaches a process for protecting a computer from hostile code, the process comprising:

- Defining at least two trust groups, each of the defined trust groups being characterized by a trust group value (col. 5, lines 25-30);
- Assigning objects and processes in the computer to one of said trust groups, irrespective of the rights of a user of said computer (col. 5, lines 19-25);

- Defining at least two object types (col. 4, line 61 through col. 5, line 18);
- **Defining a plurality of operation types** (col. 6, lines 40-43 and col. 6, line 66 through col. 7, line 3);
- Assigning an object type to each of the objects (col. 4, lines 61-64);
- Defining **a plurality of** action rules, each **of the action rules listing a** combination of **an operation type from the plurality of operation types, an action,** and object type (fig. 4-7 and col. 5, line 46 through col. 7, line 24); and
- Upon an access request **of an operation type** by a requesting process to a target object, **comparing the trust group value of the trust group of the process to the trust group value of the trust group of the object** (col. 5, lines 58-66); and
- **When the trust group value of the trust group of the process is higher than the trust group value of the trust group of the object, inspecting the trust group of the process to obtain a matching action rule listing the same operation type of the access request and the same object type of the target object and, once a matching action rule is obtained,** performing the action indicated by the **matching** action rule (fig. 4 and col. 5, lines 46 through col. 6, line 21); **and**
- **When the trust group value of the trust group of the process is smaller than the trust group value of the trust group of the object, inspecting the trust group of the object to obtain a matching action rule listing the same operation type of the access request and the same object type of the target**

object and, once a matching action rule is obtained, performing the action indicated by the matching action rule (fig. 7 and col. 6, line 66 through col. 7, line 24).

Keronen does not teach **a FromLower rules list pointer, and a ToLower rules list pointer, each of the action rules corresponding to at least one of the FromLower or ToLower rules list pointers, and inspecting all action rules corresponding to the ToLower/FromLower action rules list pointer.**

Edwards et al. teaches **a FromLower rules list pointer, and a ToLower rules list pointer** (col. 10, lines 29-36), **each of the action rules corresponding to at least one of the FromLower or ToLower rules list pointers** (col. 10, lines 29-36), and inspecting **all action rules corresponding to the ToLower/FromLower action rules list pointer** (fig. 3d through fig. 3g).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine inspecting all rules referenced by a set of pointers, as taught by Edwards et al., with the method of Keronen. It would have been obvious for such modifications because inspecting all rules ensures that the appropriate rule, based on the supplied information, is used.

Regarding claim 2, Keronen as modified by Edwards et al. wherein a process is assigned upon creation to the trust group assigned to the passive code from which the process is created (see col. 4, lines 46-60 of Keronen).

Regarding claim 3, Keronen as modified by Edwards et al. teaches further comprising changing the trust group of the process if the trust group value of the process is greater than the trust group value of the object (see col. 5, lines 25-26 of Keronen).

Regarding claim 4, Keronen as modified by Edwards et al. teaches further comprising changing the trust group of said object after performing said action (see col. 6, lines 1-5 of Keronen).

Regarding claim 5, Keronen as modified by Edwards et al. teaches further comprising, upon creation of an object by a process, assigning said created object to the trust group of said process (see col. 4, lines 46-60 of Keronen).

Regarding claim 6, Keronen as modified by Edwards et al. teaches **wherein the object types comprise executable file, document file, and registry key** (see col. 4, lines 61-66 of Keronen).

Regarding claim 8, Keronen as modified by Edwards et al. teaches further comprising assigning said process to the trust group of said object if the trust group of said process is higher than the trust group of said object (see fig. 6 of Keronen).

Regarding claim 9, Keronen as modified by Edwards et al. teaches wherein upon a restart of said process, the trust group of said process reverts to the original trust group of the object from which the process was created (the entities are created in software that reverts back to its original values when restarted).

Regarding claim 10, Keronen as modified by Edwards et al. teaches **wherein each of the action rules further lists a rule priority** (see abstract of Edwards et al., temporary nodes are inserted before (higher priority) modified nodes to preserve existing paths).

Regarding claims 11 and 16, Keronen as modified by Edwards et al. teaches wherein said object types comprise passive code and executable code (see col. 4, lines 61-66 of Keronen).

Regarding claims 12 and 15, Keronen as modified by Edwards et al. teaches wherein said operation types comprise open, read, create, modify, and delete (see fig. 6 and fig. 7 of Keronen).

Regarding claim 13, Keronen teaches a computer-readable medium comprising computer readable instructions for protecting a computer from hostile code, the instructions causing the computer to:

- Define a plurality of trust group values (col. 5, lines 25-30);
- Identify objects and processes within the computer (col. 4, line 61 through col. 5, line 18);
- Define a table of at least two trust groups, wherein each trust group comprise one trust group value and said first and second rule sets (col. 4, lines 61-64); and
- Assign objects and processes in the computer to one of said trust groups irrespective of the rights of a user of said computer (col. 5, lines 19-25);

Whereby upon operation of a process over an object, the computer is configured to:

- Compare a trust group value of the process with a trust group value of the object and determine whether to allow the operation by following the rules of said first rule set if the trust group value of the process is not smaller than the trust group of the object and following the rules of said second rules set if the trust group value of the process is smaller than the trust group value of the object (fig. 4-7 and accompanying description).

Keronen does not teach defining a first and second rule sets, each of said rule sets comprising a plurality of rules defining an action based on an operation type.

Edwards et al. teaches defining a first and second rule sets, each of said rule sets comprising a plurality of rules defining an action based on an operation type (fig. 3d through fig. 3g).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine defining multiple rule sets where each rule sets comprises a plurality of rules, as taught by Edwards et al., with the medium of Keronen. It would have been obvious for such modifications because inspecting all rules ensures that the appropriate rule, based on the supplied information, is used.

Regarding claim 14, Keronen as modified by Edwards et al. teaches further comprising instructions causing the computer to: define a table of types of at least two types of objects, the objects in the computer being assigned one type (see col. 4, line 61 through col. 5, line 18 of Keronen); and wherein said plurality of rules defines said actions further based on the type of said object (see fig. 4-7 of Keronen).

Regarding claims 19 and 21, Keronen as modified by Edwards et al. teaches wherein the computer is operatively coupled to a network, the network including a server, the table of trust groups/rules is stored in said server (see col. 7, lines 52-54 of Keronen).

Regarding claim 23, Keronen teaches a computer comprising:

- A random access memory (fig. 9, ref. num 906);
- A non-volatile memory (fig. 9, ref. num 912);
- A processor coupled to said RAM and said non-volatile memory (fig. 9, ref. num 904);
- Wherein said non-volatile memory comprises:
  - A list of object types (col. 4, line 61 through col. 5, line 18);
  - A list of rules, each rule defining an action based on an object type **and operation type** (fig. 4-7, each figure represents a different operation type, i.e., reading, writing);
  - A list of object trust groups, each trust group defining an object trust value and coupled to at least one of said rules (col. 5, lines 25-30);
  - A plurality of objects, each of said objects having an object type and assigned to one of said trust groups (col. 5, lines 19-25); and
- Wherein when a process is created in said RAM from an originating object of one of said objects, said processor assigns to said process a process trust value equal to the object trust value of said originating object **and enters the process trust value in said process trust list** (fig. 4-7).

Keronen does not teach **wherein upon start of the computer, a process trust list is initiated in said RAM**.

Edwards et al. teaches **wherein upon start of the computer, a process trust list is initiated in said RAM** (col. 7, lines 57-60).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine placing a process trust list in RAM upon start of the computer, as taught by Edwards et al., with the computer of Keronen. It would have been obvious for such modifications because items that are placed in RAM during start up of a computer are readily accessible by the computer for initial processing.

Regarding claim 24, Keronen as modified by Edwards et al. teaches further comprising a controller receiving operation requests from said process to be performed on a target object of one of said objects and, upon receiving said requests said controller access said list of object trust groups, list of rules, and list of object type to determine whether to allow the operation (see fig. 1, ref. num 104 and col. 6, lines 1-5 of Keronen).

Regarding claim 26, Keronen as modified by Edwards et al. teaches wherein when the controller allows the operation request but the process trust value is lower than the target object trust value, said processor resets the process trust value equal to that of the target object trust value (see fig. 6 of Keronen).

Response to Arguments

5. Applicant's arguments for independent claims 1 and 23 are moot in view of the new ground of rejection.

6. Regarding independent claim 13, applicant argues that Keronen does not teach defining first and second rules, defining a table of at least two trust group values, and determining whether to allow operations (page 10).

Applicant's arguments for claim 13 fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

Conclusion

7. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

BH

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

3/28/07